ACTIVACIÓN Y OPERACIÓN DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN DE TIC

	Elaboró:	Revisó:	Autorizó:
Puesto	Jefatura de Gestión de Arquitectura e Infraestructura Tecnológica	Subdirección de Tecnologías de la Información y Comunicaciones	Dirección General
Firma			

1. Propósito

Administrar de manera oportuna el ciclo de vida de los incidentes de seguridad que requiera de la intervención del "**Equipo de Respuesta a Incidentes de Seguridad de TIC (ERISC)**", que se presenten en el Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra.

2. Alcance

Aplica para todos los servicios de tecnologías de la información y comunicaciones del Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra, que requieran de la atención inmediata ante un incidente de seguridad que impacte en la disponibilidad, integridad y confidencialidad de la información resguardada y almacenada en los activos de TIC.

3. Responsabilidades

- **Líder del ERISC**: Supervisar la difusión y la aplicación de la Guía Técnica de Respuesta a Incidente, convocar al ERISC, así como verificar el establecimiento y actualización del Repositorio de Incidentes de Seguridad, recibir reportes sobre la ejecución de las acciones de resolución de incidentes y establecer los mecanismos de comunicación efectivos para convocar al ERISC, supervisar el cierre de incidentes y que se integren al Repositorio de Incidentes de Seguridad e informar al Responsable de la Seguridad de la Información en el Instituto, sobre los incidentes de seguridad de la información de TIC y su solución.

- **Líder suplente del ERISC**: Coordinar la elaboración, difusión y aplicación de la Guía Técnica de Respuesta a Incidentes, verificar el establecimiento y actualización del Repositorio de Incidentes de Seguridad, en sustitución del Líder del ERISC, convocar al Equipo, supervisar la ejecución de las acciones de resolución de incidentes y establecer los mecanismos de comunicación efectivos para convocar al ERISC, participar activamente en la aplicación de los procedimientos de atención a incidentes con el resto del Equipo, realizar el cierre de incidentes y verificar que se integren al Repositorio de Incidentes de Seguridad, e informar al Líder del ERISC sobre los incidentes de seguridad de la información de TIC y su correspondiente atención y solución.

- **Analista de Incidentes de seguridad**: Colaborar activamente en la elaboración de la Guía técnica de Respuesta a Incidentes, proponer los mecanismos de monitoreo y detección de incidentes conforme a los procesos y sistemas de su responsabilidad, participar activamente en la aplicación de los procedimientos de atención a incidentes con el resto del Equipo y en el caso de requerir, tomar decisiones sobre la recuperación de la infraestructura critica que haya tenido la falla, la deberán tomar en forma conjunta las Jefaturas de Gestión de Arquitectura e Infraestructura Tecnológica, Gestión y Desarrollo de soluciones Tecnológicas, Gestión y Operación de Servicios y Gestión Estratégica , además de facilitar la información necesaria para el registro y/o actualización de los incidentes en el repositorio.

4. Políticas de operación y normas.

PO1-STIC-30. Un incidente de seguridad que requiera la intervención del ERISC definido en el formato del Equipo de Respuesta a Incidente (F01-PR-STIC-30) deberá ser notificado inmediatamente al Líder del ERISC y/o al Líder suplente del ERISC.

PO2-STIC-30. El procedimiento de atención a incidentes de seguridad de la información deberá ser activado únicamente por los integrantes del ERISC.

PO3-STIC-30. Los documentos relacionados a los incidentes de seguridad de la información de TIC, tales como: Guía técnica de respuesta a incidentes, Registro de datos del incidente y su solución, Bitácoras de Operación, Notas Informativas, así como los Reportes de incidentes al Responsable de la Seguridad de la Información, será almacenada en el Repositorio de Incidentes de Seguridad. Dicho repositorio contará con controles de acceso para los miembros del equipo conforme al rol desempeñado y al tema específico de su atención.

PO4-STIC-30. Mantener informada a la Mesa de Servicios en el ciclo del incidente de seguridad de la información de TIC.

PO5-STIC-30. Los incidentes de seguridad de la información deberán ser reportados al Responsable de la Seguridad de la Información del INRLGII.

PO6-STIC-30. El cierre de los incidentes solo podrá ser realizado por el Líder o, en su caso el Suplente del Equipo de Respuesta a Incidentes de Seguridad de la Información de TIC.

PO7-STIC-30. Mantener actualizada la información del Repositorio de riesgos, con la siguiente información:

a) Análisis de Riesgos (F02-PR-STIC-30).
b) La información de la Directriz rectora para la administración de riesgos (F04-PR-STIC-30).
c) El Programa de contingencia a los de riesgos (F03-PR-STIC-30).
d) Documento de identificación de amenazas (F08-PR-STIC-30)

5. Descripción del procedimiento:

N°	RESPONSABLE	ACTIVIDAD
1.	**Analista de incidentes de seguridad**	Identificar un incidente de seguridad de TIC que debe atender el ERISC.
2.		Informar al Líder del ERISC y/o Líder suplente del ERISC del incidente
3.	**Líder del ERISC/Líder suplente del ERISC**	Asignar a los **Analistasde incidentes de seguridad** correspondientes para la atención del incidente de acuerdo al Programa de contingencia a los Riesgos (F03-PR-STIC-30).

N°	RESPONSABLE	ACTIVIDAD
4.	**Analista de incidentes de seguridad**	Realizar un análisis exhaustivo del incidente en colaboración con los coordinadores de los diferentes departamentos de la STIC.
5.	**Analista de incidentes de seguridad**	Ejecutar acciones de contención, corrección y de ser necesario, se apoyará con los responsables de los Dominios Tecnológicos y representantes técnicos de las empresas proveedoras de los servicios de TIC para su solución. ¿Se solucionó el incidente? Si: Pasar a la actividad 7. No: Realiza una investigación técnica para la contención del incidente e informar a la Mesa de Servicios el tiempo estimado de solución. Pasar a la actividad 6.
6.	**Líder suplente del ERISC.**	Realiza el monitoreo del avance de la solución del incidente con los Analistas de incidentes de seguridad involucrados. ¿Se solucionó el incidente? Si: Pasa a la actividad 7. No: Pasar a la actividad 5.
7.	**Analista de incidentes de seguridad**	Elabora reporte de las acciones realizadas de la solución del incidente e integra la información en el Repositorio de Incidentes de Seguridad.
8.	**Analista de incidentes de seguridad**	Actualizar el documento de Directriz de Administración de Riesgos (F07-PR-STIC-30) para establecer controles que permitan minimizar el impacto en caso del algún incidente.
9.		Termina Procedimiento

6. Documentos de referencia:

DOCUMENTO	CODIGO
NMX-CC-9001-IMNC-2015 ISO 9001:2015 Sistemas de Gestión de la Calidad	N/A
Manual de Gestión de la Calidad	MGC-DG-01
Control de Documentos y Registros	PR-SGC-01
Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y	Interno

Comunicaciones y Seguridad de la Información (MAAGTICSI)	

REGISTRO	TIEMPO DE CONSERVACIÓN	RESPONSABLE DE CONSERVACIÓN	CODIGO
Equipo de respuesta a incidentes de seguridad de TIC(ERISC)	3 años	Jefatura de Departamento de Gestión de Arquitectura e Infraestructura Tecnológica	F01-PR-STIC-30
Análisis de Riesgos	3 años	Jefatura de Departamento de Gestión de Arquitectura e Infraestructura Tecnológica	F02-PR-STIC-30
Programa de contingencias a los riesgos	3 años	Jefatura de Departamento de Gestión de Arquitectura e Infraestructura Tecnológica	F03-PR-STIC-30
Directriz de administración de riesgos	3 años	Jefatura de Departamento de Gestión de Arquitectura e Infraestructura Tecnológica	F04-PR-STIC-30
Directriz rectora de respuesta a incidentes.	3 años	Jefatura de Departamento de Gestión de Arquitectura e Infraestructura Tecnológica	F07-PR-STIC-30
Documento de identificación de Amenazas	3 años	Jefatura de Departamento de Gestión de Arquitectura e Infraestructura	F08-PR-STIC-30

		Tecnológica	

7. Glosario

TIC: Tecnologías de la Información y Comunicaciones.

STIC: Subdirección de Tecnologías de la Información y Comunicaciones.

DGAIT: Departamento de Gestión de Arquitectura e Infraestructura Tecnológica.

Incidente: Cualquier evento que no forma parte de la operación estándar de un servicio y que puede causar una interrupción o una reducción de la calidad del mismo.

Activos de TIC: Los programas de cómputo, bienes informáticos, soluciones tecnológicas, sistemas o aplicativos, sus componentes, medios de transmisión y comunicación, las bases de datos o archivos electrónicos y la información contenida en éstos.

Analista Especializado: Es el personal experto en la atención o solución de uno o más servicios proporcionados por la STIC (colaboradores de la mesa de servicio,ingenieros de servicios de infraestructura para voz, datos y edificio inteligente, e ingeniero de arquitectura para cambios y configuraciones, arquitecto-diseñador o desarrollador-integrador o proveedor).

ERISC: Equipo de Respuesta a Incidentes de Seguridad de TIC.
Incidentes de Seguridad: Cualquier Evento provocado por un agente interno o externo que modifica o daña la Infraestructura y la información.

8. Control de cambios

Revisión	Descripción del cambio	Fecha
01	Actualización de la imagen institucional, actualización del nombre del instituto	JUN 15
02	Transición del SGC de la Norma ISO 9001:2008 a la Norma ISO 9001:2015	MAY 18
03	Actualización de Imagen Institucional	DIC 20